CLAIMS

We claim:

1. A method of enforcing a policy on a computer network comprising the steps of: in response to an attempt by a user to access a resource on the network, determining a group to which the user belongs; and, based on the determined group, selecting an authorization parameter, wherein the authorization parameter is usable to grant or deny access to the resource in accordance with the policy.

2. The method of claim 1, wherein the user is attempting to access the resource over a network link, further comprising the steps of: evaluating the link to determine a characteristic of the link; and selecting the authorization parameter based on the determined characteristic.

3. The method of claim 1, wherein the selecting step further comprises the step of selecting a profile based on the determined group, wherein the authorization parameter is contained in the profile.

4. The method of claim 1, wherein the determining step further comprises the step of referencing a user object corresponding to the user, wherein the user object has a group attribute representative of the group.

5. The method of claim 3, further comprising the steps of: adding an override attribute associated with the user to the profile; and determining whether to admit or deny access to the resource based on the override attribute.

6. The method of claim 1, wherein the authorization parameter is associated with a policy statement, wherein the selecting step further comprises the steps of: evaluating the policy statement based on the determined group; and if the policy statement is evaluated to be true, selecting the authorization parameter.

7. The method of claim 1, wherein the authorization parameter represents a time of day at which the user is permitted access to the network.

8. The method of claim 1, wherein the authorization parameter represents a day of the week during which the user is permitted access to the network.

9. The method of claim 1, wherein the authorization parameter represents a phone number that may be called by the user.

10. The method of claim 1, wherein the authorization parameter represents a phone number from which the user is permitted to access to the network.

11. A method of enforcing a policy on a computer network comprising the steps of: in response to an attempt by a user to access the network from a computer,

determining a group to which the user belongs; and, based on the determined group, selecting a communication parameter, wherein the communication parameter is usable to configure a data path between the computer and the network in accordance with the policy.

12. The method of claim 11, further comprising the steps of: evaluating a link over which the computer is communicating to determine a characteristic of the link; and selecting the communication parameter based on the determined characteristic.

13. The method of claim 11, wherein the selecting step further comprises the step of selecting a profile based on the determined group, wherein the communication parameter is contained in the profile.

14. The method of claim 11, wherein the determining step further comprises the step of referencing a user object corresponding to the user, wherein the user object has a group attribute representative of the group.

15. The method of claim 13, further comprising the steps of: adding an override attribute associated with the user to the profile; and configuring the data path according to the override attribute.

16. The method of claim 11, wherein the communication parameter is associated with a policy statement, wherein the selecting step further comprises the steps of:

evaluating the policy statement based on the determined group; and if the policy statement is evaluated to be true, selecting the communication parameter.

17. The method of claim 11, wherein the communication parameter represents the quality of service of the data path.

18. The method of claim 11, wherein the communication parameter represents a media type for the data path.

19. The method of claim 1, wherein the communication parameter represents an IP address for the data path.

20. The method of claim 1, wherein the communication parameter represents an encryption level for data traveling on the data path.

21. A computer-readable medium having inscribed thereon a data structure, the data structure comprising: a policy statement expressing an implementation of an policy for a computer network, the statement conditioned on a group to which a user communicating with the network over a data path belongs, wherein the policy statement is usable by the network to obtain an authorization parameter usable to grant or deny access to a resource on the network in accordance with the policy.

22. A computer-readable medium having inscribed thereon a data structure, the data structure comprising: a policy statement expressing an implementation of an policy for a computer network, the statement conditioned on a group to which a user communicating with the network over a data path belongs, wherein the policy statement is usable by the network to set a communication parameter usable to configure the data path in accordance with the policy.

23. A computer network comprising: a network access server for granting or denying access to a resource on the network from a computer according to an authorization parameter; a policy server linked for communication with the network access server, wherein the policy server provides the authorization parameter to the network access server based on a group to which the user belongs; and a directory server linked for communication with the policy server, the directory server having an object corresponding to the user, the object having an associated group attribute, the group attribute being usable by the policy server to determine the group to which the user belongs.

24. A computer network comprising: a network access server for configuring a data path between a computer and the network according to a communication parameter, wherein the data path enables a user at the computer to communicate with the network; a policy server linked for communication with the network access server, wherein the policy server provides the communication parameter to the network access server based on a group to which the user belongs; and a directory

server linked for communication with the policy server, the directory server having an object corresponding to the user, the object having an associated group attribute, the group attribute being usable by the policy server to determine the group to which the user belongs.

25. A computer-readable medium having computer-executable instructions for performing steps comprising: prompting a user to select a group on which to base a policy statement, the statement being representative of a policy for a computer network; prompting the user to select an authorization parameter to associate with the group; and, in response to the selections, creating the policy statement such that the group represents a condition of the policy statement and the authorization parameter represents the fulfillment of the condition, the authorization parameter being usable to grant or deny access to a resource on a network by a computer in communication with the network in accordance with the policy.

26. A computer-readable medium having computer-executable instructions for performing steps comprising: prompting a user to select a group on which to base a policy statement, the statement being representative of a policy for a computer network; prompting a user to select a communication parameter to associate with the group; and, in response to the selections, creating the policy statement such that the group represents a condition of the policy statement and the communication parameter represents the fulfillment of the condition, the communication parameter

being usable to configure a data path between a computer and the network in accordance with the policy.

27. A computer-readable medium having computer-executable instructions for performing steps comprising: in response to an attempt by a user to access a resource on a network, determining a group to which the user belongs; and, based on the determined group, selecting an authorization parameter, wherein the authorization parameter is usable to grant or deny access to the resource in accordance with a policy of the network.

28. A computer-readable medium having computer-executable instructions for performing steps comprising: in response to an attempt by a user to access a network from a computer, determining a group to which the user belongs; and, based on the determined group, selecting a communication parameter, wherein the communication parameter is usable to configure a data path between the computer and the network in accordance with a policy of the network.

29. A method of enforcing a policy on a computer network comprising the steps of: in response to an attempt by a user to access the network through a communication medium, determining a group to which the user belongs; determining the medium type and, based on the determined group and the medium type, selecting an action, wherein the action is usable to grant or deny access to the network in accordance with the policy.

30. A method of enforcing a policy on a computer network comprising the steps of: in response to an attempt by a user to access a network over a dial up link using a called number, determining a group to which the user belongs; determining the called number of the dial up link and, based on the determined group and the number, selecting an action, wherein the action is usable to grant or deny access to the network in accordance with the policy.

31. A computer-readable medium having computer-executable instructions for performing the steps of: in response to an attempt by a user to access a computer network through a communication medium, determining a group to which the user belongs; determining the medium type and, based on the determined group and the medium type, selecting an action, wherein the action is usable to grant or deny access to the network in accordance with a policy of the network.

32. A computer-readable medium having computer-executable instructions for performing the steps of: in response to an attempt by a user to access a computer network over a dial up link using a called number, determining a group to which the user belongs; determining the called number of the dial up link and, based on the determined group and the number, selecting an action, wherein the action is usable to grant or deny access to the network in accordance with a policy of the network.